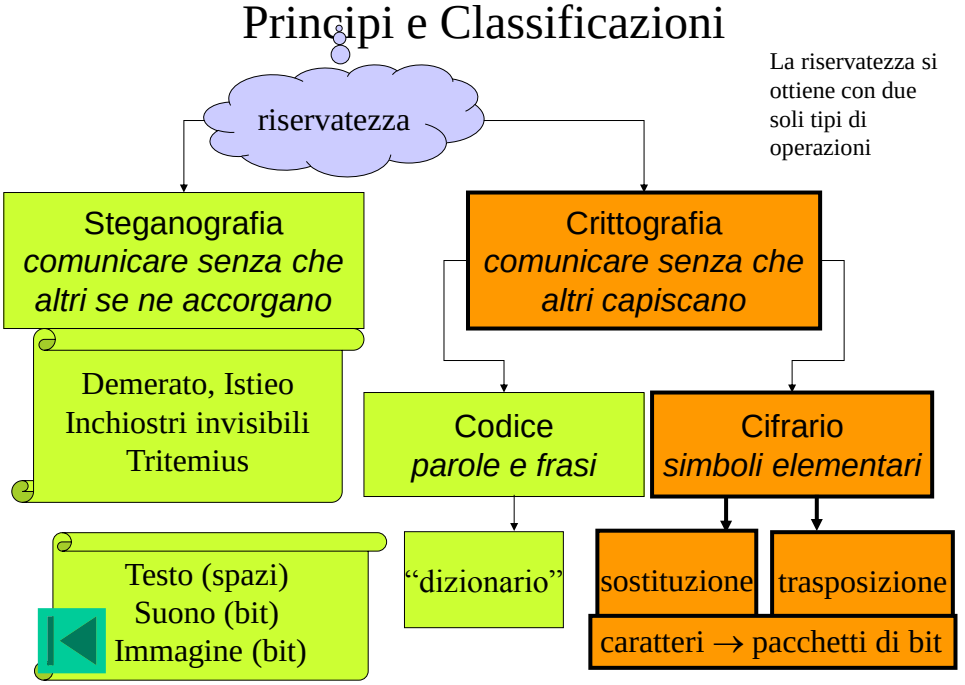
Crittologia classica

Crittografia classica: la storia

- 1900 a.c. Egitto: geroglifici non standard
- 1500 a.c Mesopotamia: Formula con molte interpretazioni
- 500 a.c Israele: Codice ATBASH per il libro di Geremia
- 500 a.c. Plutarco: Scitale degli Spartani
- 50 a.c. Svetonio: Cifrario di Giulio Cesare
- 300 d.c. Kama Sutra
- 725 d.c. Abu al Yahmadi: sostituzione e trasposizione
- XV°-XVI° sec: sostituzione polialfabetica
- 1917 Macchina di Vernam
- 1930-40 Macchine cifranti: Schrebius, Hagelin
- 1940-45 Macchine per crittanalisi: Turing, Shannon

Principi e Classificazioni



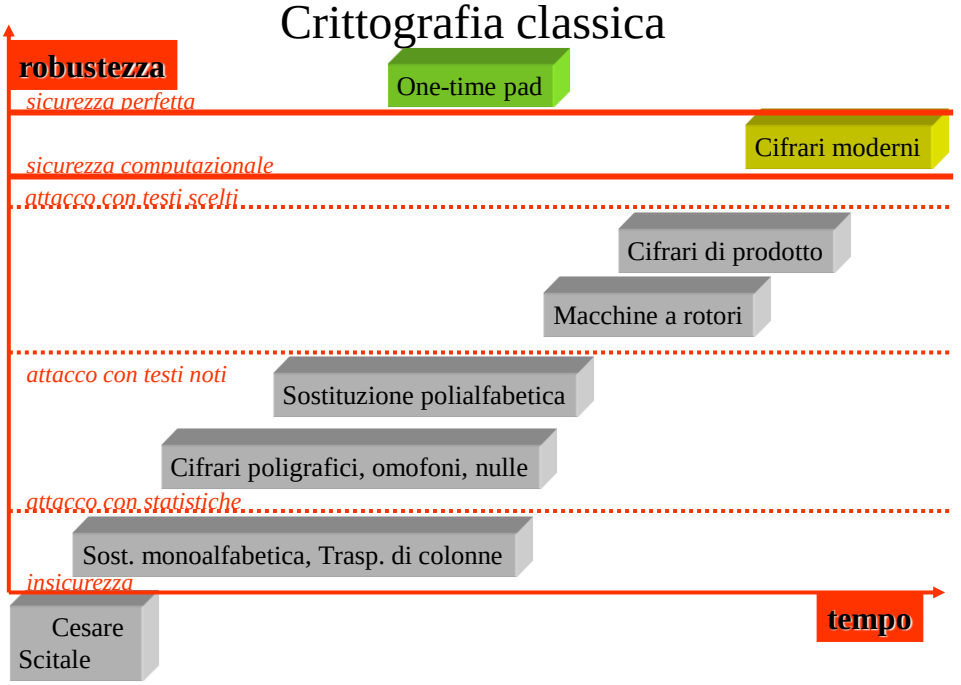
Decrittazione

Obiettivi dell'intruso:
•il testo in chiaro
•la chiave

ATTACCO	CONOSCENZE DELL'INTRUSO
con solo testo cifrato *ciphertext-only*	**linguaggio usato nel testo in chiaro e statistiche sull'occorrenza dei simboli**
con testo in chiaro noto *known plaintext*	**coppie di testo cifrato intercettato e testo in chiaro corrispondente**
con testo in chiaro scelto *chosen plaintext*	**testi cifrati corrispondenti a testi in chiaro di sua scelta**
con testo cifrato scelto *chosen ciphertext*	**testi in chiaro corrispondenti a testi cifrati di sua scelta**

Pericolosità *e quindi* **Robustezza**

Crittografia classica



Crittografia classica: la sostituzione monoalfabetica

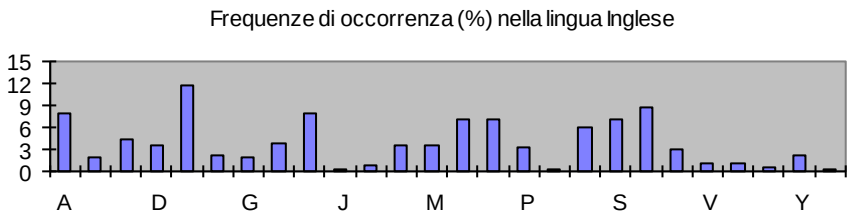
regola di sostituzione (o chiave)

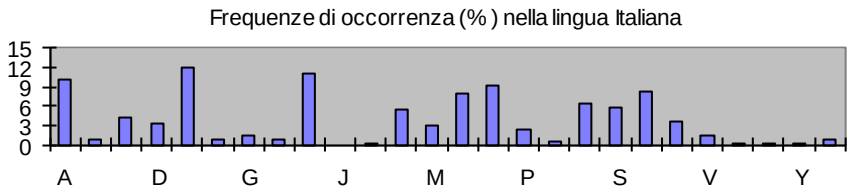
A	B	C	D	E	F	G	H	I	L	M	N	O	P	Q	R	S	T	U	V	Z
Q	E	M	R	F	Z	T	B	L	U	P	O	N	H	A	S	C	G	V	D	I

testo in chiaro:CRITTOGRAFIA
testo cifrato: MSLGGNTSQZLQ

$26! = 4 \times 10^{26}$

Statistiche dei caratteri





Probabilità di occorrenza

Statistiche di digrammi e trigrammi

Lingua inglese	
TH	3,16%,
IN	1,54%
ER	1,33%
RE	1,3%
ecc.	
THE	4,72
ING	1,42
ecc.	

•un linguaggio naturale è ridondante
•la probabilità di occorrenza di stringhe corte è indipendente dal testo
•in un testo lungo le frequenze di occorrenza approssimano le probabilità

Il punto debole della monoalfabetica

Le proprietà statistiche di ogni carattere del testo in chiaro vengono trasferite immutate sul carattere che lo sostituisce nel testo cifrato

Un grande spazio delle chiavi può non servire a nulla!

Crittografia classica: la trasposizione di colonne

Tabella **5 × 8** e chiave **76518234**:

Testo in chiaro: **ALLE PROSSIME ELEZIONI MI PRESENTO**

A	L	L	E	P	R	O	S
S	I	M	E	E	L	E	Z
I	O	N	I	M	I	P	R
E	S	E	N	T	O	X	X

Ordine: 7 6 5 1 8 2 3 4

Statistiche dei digrammi e dei trigrammi alterate dall'operazione di affiancamento delle colonne

Simboli di riempimento

Testo cifrato: EEIN RLIO OEPX SZRX LMNELIOSASIE

Ogni carattere del testo cifrato mantiene le proprietà statistiche che ha nel linguaggio naturale, quindi poco utile. Quale info sfrutto? Le statistiche dei digrammi nel linguaggio naturale permettono invece di individuare quali sequenze di due simboli non sono naturali ma derivano dalla scrittura in colonne del testo in chiaro

Crittografia classica: la trasposizione di colonne

Tabella **5 × 8 (PxQ)** e chiave **76518234**:

Ordine:	1	2	3	4	5	6	7	8
	E	R	O	S	L	L	A	P
	E	L	E	Z	M	I	S	E
	I	I	P	R	N	O	I	M
	N	O	X	X	E	S	E	T
Chiave:	7	6	5	1	8	2	3	4

Ora si spostano le colonne in modo che l'indice di ricezione corrisponda ai numeri nella chiave

Mascheramento della ridondanza

equiprobabilità di occorrenza di ogni simbolo del testo cifrato

CRITTOGRAFIA CLASSICA
- **Eliminazione delle spaziature e dei segni di interpunzione**
- **Nulle**: caratteri non significativi
- **Omofoni**: più simboli per i caratteri più frequenti
- **Cifrari poligrafici**: cifratura di due o tre caratteri consecutivi
- **Cifrari polialfabetici**: trasformazioni variabili

CRITTOGRAFIA MODERNA usa spesso la sostituzione
- almeno 8 caratteri alla volta (64 bit)
- trasformazione dipendente da tutti i "blocchi" precedenti
- Compressione senza perdita
- RC4: "*non bisogna mai cifrare troppo testo con la stessa chiave*"

Playfair Cipher (sostituzione di digrammi)

CHIAVE

L	Z	Q	C	P
A	G	N	O	U
R	D	M	I	F
K	Y	H	V	S
X	B	T	E	W

o si elimina la doppia o carattere improbabile

- J sostituito da I

Il digramma in chiaro identifica la diagonale di un rettangolo: il digramma cifrato è dato dai caratteri posti all'estremità dell'altra diagonale

- AI → RO
- RI → DF

Se i digrammi sulla stessa riga -> quelli nelle casella alla destra

- LP → ZL
- AK→ RX

Se i digrammi sulla stessa colonna -> quelli nelle casella sottostanti

- "doppia": regole varie

La sostituzione polialfabetica (Vigenere)

testo

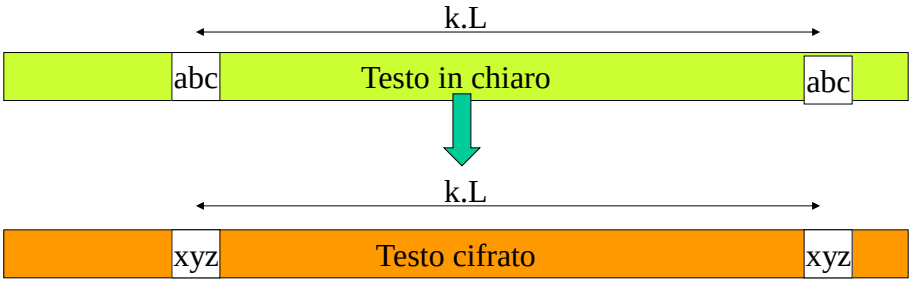
chiave

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYZAB
DEFGHIJKLMNOPQRSTUVWXYZABC
.....
ZABCDEFGHIJKLMNOPQRSTUVWXY

Chiave: CIAO
testo in chiaro : DOMANI NON POSSO
Cifratura:

C	I	A	O	C	I	A	O	C	I	A	O	C	I	
D	O	M	A	N	I	N	O	N	P	O	S	S	O	
F	Z	M	O	P	S	N	C	P	A	O	H	U	Z	

Test di Kasiski



Chiave: ciao

Testo in chiaro: domani non puo domani deve andare a scuola

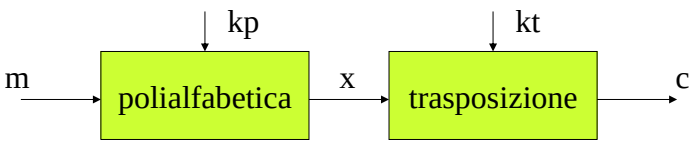
Due poligrammi identici presenti nel testo in chiaro ad una distanza uno dall'altro pari a un multiplo della lunghezza della chiave sono necessariamente sostituiti da poligrammi identici nel testo cifrato. Per sapere con buona probabilità la lunghezza di una chiave occorre:

1: ricerca nel cifrato di sequenze identiche
2: annotazione delle distanze
3: fattorizzazione e scelta delle distanze con un fattore comune
4: L = MCD

Accorgimenti utili

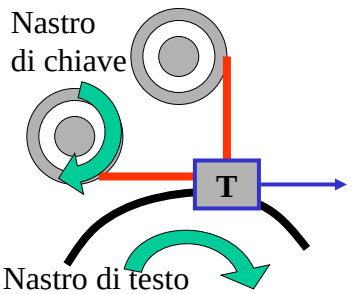
- R12: "*chiave lunga e scelta a caso"*
- R25: " *mai archiviare insieme testi cifrati e decifrazioni*".
- R26: " *mai lasciare incustodite macchine pronte per cifrare/decifrare*"
- R27: "*ogni simbolo del blocco in chiaro deve influire sul valore di tutti i simbolo del blocco cifrato*"

Iª Guerra Mondiale: **sopracifratura**



Il cifrario Vernam
One time pad

Il Cifrario di Vernam (1917)



Telegrafo di Vernam

- *codifica binaria (5 bit) codice di baudot a 32 bit per telescriventi)*
- *chiave lunga quanto il testo*

•Ogni carattere cifrato aggiungendo (somma modulo 2 – funzione invertibile) un carattere oscurante

•Addizione eseguiti sui singoli bit costitutivi il carattere

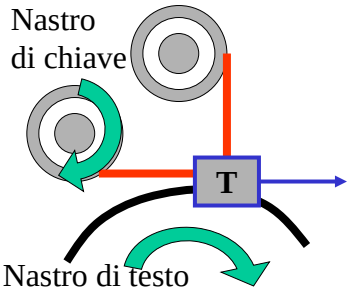
•Per la decrittazione si somma al carttere del testo cifrato di nuovo il carattere oscurante

es. T (00001) carattere in chiaro
\+ (addizione modulo 2 , XOR)
C (01110) carattere oscurante
V (01111) carattere cifrato

Binary value	Letters	Figures
00011	A	-
11001	B	?
01110	C	:
01001	D	$
00001	E	3
01101	F	!
11010	G	&
10100	H	STOP
00110	I	8
01011	J	'
01111	K	(
10010	L	)
11100	M	.
01100	N	,
11000	O	9
10110	P	0
10111	Q	1
01010	R	4
00101	S	BELL
10000	T	5
00111	U	7
11110	V	;
10011	W	2
11101	X	/
10101	Y	6
10001	Z	"
00000	n/a	n/a
01000	CR	CR
00010	LF	LF
00100	SP	SP
11111	LTRS	LTRS
11011	FIGS	FIGS

Figure 3. The Baudot Code Set

Il Cifrario di Vernam (1917)



Telegrafo di Vernam
- *codifica binaria (5 bit)*
- *chiave lunga quanto il testo*

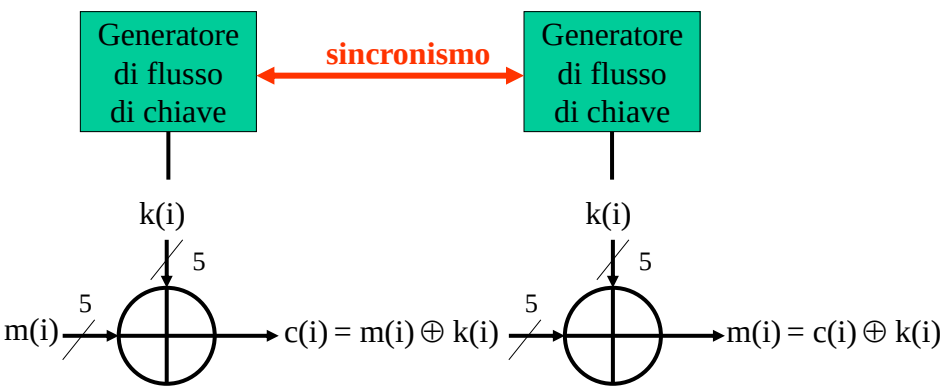
	Chiave							
Testo	000	001	010	011	100	101	110	111
000	000	001	010	011	100	101	110	111
001	001	000	011	010	101	100	111	110
010	010	011	000	001	110	111	100	101
011	011	010	001	000	111	110	101	100
100	100	101	110	111	000	001	010	011
101	101	100	110	111	001	000	011	010
110	110	111	100	101	010	011	000	001
111	111	110	101	100	011	010	001	000

8 righe: 8 permutazioni di {0,1,..,7}

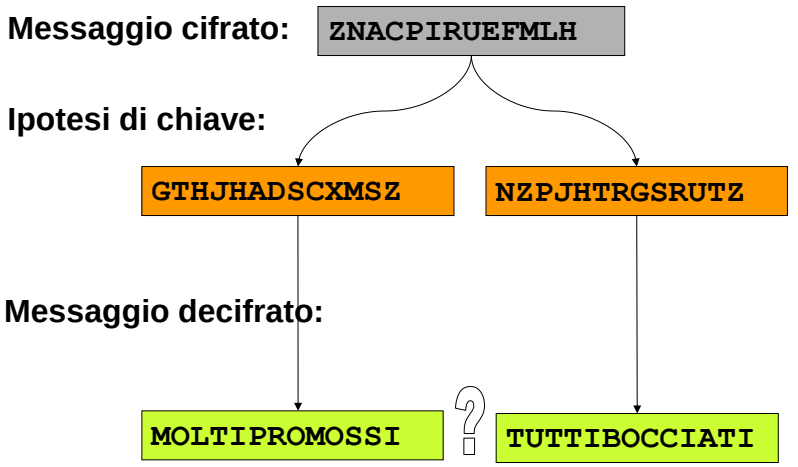
Mauborgne: *chiave scelta a caso e usata una sola volta*

Polialfabetica con *running key*

Il Cifrario di Vernam-Mouborgne



One-time pad: inviolabile con attacco passivo



Per trasmettere un messaggio riservato su un canale insicuro bisogna concordare una chiave altrettanto lunga su un canale sicuro

Problemi di one-time pad

•Accordo riservato su molte chiavi molto lunghe

•Uguale probabilità di occorrenza dei simboli di chiave

•Ricezione di tutto il testo cifrato in ordine

Bletchley Park

Spie russe

Telefono rosso

Attacco attivo

•Impiego di meccanismi di autenticazione (H, S)

Definizioni di sicurezza per un Cifrario

SEGRETEZZA PERFETTA

Un Cifrario è detto **perfetto**, o **assolutamente sicuro**, se, dopo aver intercettato un certo testo cifrato **C**, l'incertezza *a posteriori* sul testo in chiaro **M** corrispondente è uguale all'incertezza che si aveva *a priori* , cioè prima dell'intercettazione.

SICUREZZA

Un Cifrario è **sicuro** se dato un qualsiasi testo cifrato **C**, il trovare un **M** tale che $\mathbf{E_k(M) = C}$ è **impossibile** per chi non conosce **k**.

SICUREZZA COMPUTAZIONALE

Un Cifrario è detto **computazionalmente sicuro** se il calcolare **M** da un **C** è possibile, ma richiede una potenza di elaborazione superiore a quella a disposizione dell'attaccante.

Confusione & Diffusione (C. Shannon)

La **confusione** nasconde la relazione esistente tra testo in chiaro e testo cifrato e rende poco efficace lo studio del secondo basato su statistiche e ridondanze del primo.Rende difficile prevedere che cosa Accadrà al cifrato anche modificando un solo simbolo Del testo in chiaro
La **sostituzione** è il mezzo più semplice ed efficace per creare confusione.

Cifrario composto: S&T iterato

La **diffusione** nasconde la ridondanza del testo in chiaro spargendola all'interno del testo cifrato. Si impone ad ogni simbolo del testo in chiaro di influire su molti se non tutti i simboli del testo cifrato. Difficile prevedere quali e quanti si modificano se si modifica anche un solo simbolo del testo in chiaro
La **trasposizione** è il mezzo più semplice ed efficace per ottenere diffusione

Il cifrario composto